REMARKS

Claims 1-65 are pending in this application. By this Response, arguments regarding the novelty of new claims 62-65, which were added by the reply filed on February 28, 2006, are presented. Reconsideration in view of the following remarks is respectfully requested.

I. NEW CLAIM 62 IS PATENTABLE

NEW CLAIM 62 DEPENDS DIRECTLY FROM CLAIM 18.

As discussed in the reply filed on February 28, 2006, Bisbee fails to teach or suggest a method for creating and validating at least one digital signature for an electronic authoritative record maintained in a secure environment, wherein control is maintained in the secure environment by software and at least one server, and a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, comprising "receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially complete message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the

beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce a digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 18.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document,

thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for creating and validating at least one digital signature for an electronic authoritative record maintained in a secure environment, wherein control is maintained in the secure environment by software and at least

one server, and a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, comprising "receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially complete message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce a digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital

signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 18, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method for creating and validating at least one digital signature for an electronic authoritative record maintained in a secure environment, wherein control is maintained in the secure environment by software and at least one server, and a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, comprising "receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a remote

location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially complete message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce a digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 18.

Therefore, Applicant respectfully submits that independent claim 18 is patentable over Bisbee in view of Vanstone. Likewise, new claim 62 is also patentable over Bisbee in view of Vanstone by virtue of its direct dependence from claim 18, for the reasons discussed above, and for the additional feature(s) new claim 62 recites.

II. NEW CLAIM 63 IS PATENTABLE

NEW CLAIM 63 DEPENDS DIRECTLY FROM CLAIM 49.

As discussed in the reply filed on February 28, 2006, Bisbee fails to teach or suggest a system for creating and validating at least one digital signature on an electronic authoritative

record that is maintained in a secure environment, wherein a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the system comprising "at least one server, connected to a network, that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes a portion of the software, wherein the software provides for: receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a person at the remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially completed message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce the digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital

signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 49.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "Vanstone discloses generating a hash (message digest) of a part (partial) of a document". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a system for creating and validating at least one digital signature on an electronic authoritative record that is maintained in a secure environment, wherein a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the system comprising "at least one server, connected to a network, that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes a portion of the software, wherein the software provides for: receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information.

wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a person at the remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially completed message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce the digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 49, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a system for creating and validating at least one digital signature on an electronic authoritative record that is maintained in a secure environment, wherein a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the system comprising "at least one server, connected to a network, that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes a portion of the software, wherein the software provides for: receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a person at the remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially completed message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at

the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce the digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 49.

Therefore, Applicant respectfully submits that independent claim 49 is patentable over Bisbee in view of Vanstone. Likewise, new claim 63 is also patentable over Bisbee in view of Vanstone by virtue of its direct dependence from claim 49, for the reasons discussed above, and for the additional feature(s) new claim 63 recites.

III. NEW CLAIM 64 IS PATENTABLE

NEW CLAIM 64 IS PATENTABLE OVER THE PRIOR ART OF RECORD

For example, as discussed in the reply filed on February 28, 2006, Bisbee fails to teach or suggest a method for creating a unique authoritative electronic record, comprising "receiving an electronic record into a repository, wherein the repository is contained on an electronic device that stores and executes software; generating a receipt, wherein the receipt includes a digital signature of the electronic record; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the supplemental information to an ending of the record; and storing the record with the prepended

receipt and the appended supplemental information as the unique authoritative record in the repository" (emphasis added), as recited in new claim 64.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "Vanstone discloses generating a hash (message digest) of a part (partial) of a document". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a

data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for creating a unique authoritative electronic record, comprising "receiving an electronic record into a repository, wherein the repository is contained on an electronic device that stores and executes software; generating a receipt, wherein the receipt includes a digital signature of the electronic record; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the supplemental information to an ending of the record; and storing the record with the prepended receipt and the appended supplemental information as the unique authoritative record in the repository" (emphasis added), as recited in new claim 64, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) teach or suggest a method for creating a unique authoritative electronic record, comprising "receiving an electronic record into a repository, wherein the repository is contained on an electronic device that stores and executes software; generating a receipt, wherein the receipt includes a digital signature of the electronic record; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the supplemental information to an ending of the record; and storing the

record with the prepended receipt and the appended supplemental information as the unique authoritative record in the repository" (emphasis added), as recited in new claim 64.

Therefore, Applicant respectfully submits that new claim 64 is patentable over Bisbee in view of Vanstone (the prior art of record).

IV. NEW CLAIM 65 IS PATENTABLE

NEW CLAIM 65 IS PATENTABLE OVER THE PRIOR ART OF RECORD

For example, as discussed in the reply filed on February 28, 2006, Bisbee fails to teach or suggest a method for obtaining a digital signature on an authoritative record stored in a secure environment, comprising "receiving a request to sign the authoritative record; computing a partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; computing a complement of the proper subset; sending the partial message digest and at least the complement of the proper subset of the authoritative record to a remote location; completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset; and creating a digital signature with the use of the message digest and a private key" (emphasis added), as recited in new claim 65.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document,

thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "Vanstone discloses generating a hash (message digest) of a part (partial) of a document". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record. Thus, Bisbee fails to teach the claimed subject matter of original claim 5.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for obtaining a digital signature on an authoritative record stored in a secure environment, comprising "receiving a request to sign the authoritative record; computing a partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the

authoritative record; computing a complement of the proper subset; sending the partial message digest and at least the complement of the proper subset of the authoritative record to a remote location; completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset; and creating a digital signature with the use of the message digest and a private key" (emphasis added), as recited in new claim 65.

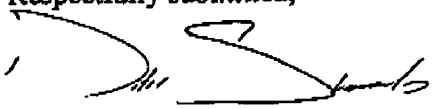
Therefore, Applicant respectfully submits that new claim 65 is patentable over Bisbee in view of Vanstone (the prior art of record).

CONCLUSION

Based on the reply filed on February 28, 2006, and the foregoing remarks, Applicant respectfully submits that claims 1-61 and new claims 62-65 are directed to allowable subject matter and that the application is in condition for allowance. Accordingly, prompt reconsideration and allowance of the application with these claims is respectfully requested.

However, if the Examiner believes there is anything further necessary to place this application in better condition for allowance, Applicant requests the Examiner telephone Applicant's undersigned representative at the number listed below.

Respectfully submitted,



Peter A. Shaddock II
Registration No. 44,331

Date: *June 8, 2006*

Bowman Green Hampton & Kelly, PLLC
501 Independence Parkway, Suite 201
Chesapeake, VA 23320-5173

Telephone: (757) 548-2323
Fax: (757) 548-2345
E-mail: pshaddock@bghklaw.net